

## REMARKS

Claims 1, 3-30, and 32-81 are pending and remain. Claims 1-29, 60-76, and 78-81 have been amended. No new matter has been entered.

The amendments present the rejected claims in better form for  
5 consideration on appeal and may be admitted pursuant to 37 C.F.R. § 1.116(b)(2).

### **Rejections under 35 U.S.C. § 101**

Claims 1, 3-29, 60-68, and 79 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Office personnel have the burden to establish a *prima facie* case that the claimed invention as a whole is directed to  
10 solely an abstract idea or to manipulation of abstract ideas or does not produce a useful result. Applicant traverses the rejection.

Claims 1, 60, and 79 now define apparatuses. Independent Claim 1 recites a key repository and an external device. The external device can include a programmer or a dedicated repeater (Spec., page 7, lines 1-3). The key repository  
15 can include a programmer, patient designator, secure database, token, or repeater, or can be included on an implantable medical device (Spec., page 10, lines 7-9). Claim 60 recites a short range interface device and an external device. The short range interface device can include devices that have the ability to communicate through a short range interface (Spec., page 13, lines 1-5). Claim 79 recites a  
20 secure server, which is a computer that runs an application, and an external device. Therefore, each of the components recited in independent Claims 1, 60, and 79 are tangible and the claimed invention as a whole falls under the statutory class for a machine.

Accordingly, a *prima facie* case of non-statutory subject matter is not  
25 present. Claims 3-29 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 61-68 are dependent on Claim 60 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. As the claimed invention is directed to statutory subject matter, withdrawal of the rejection is requested.

### **Rejections under 35 U.S.C. § 102(e) over Thompson**

Claims 1, 3, 5-10, 17-20, 27-30, 32, 34-39, 46-49, 56-61, 68-70, and 77-81

stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,027,872, to Thompson. Applicant traverses.

A claim is anticipated under 35 U.S.C. § 102(e) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. MPEP 2131. Further, a reference may be “relied upon for all that it would have reasonably have suggested to one having ordinary skill in the art.” MPEP 2123. Thompson fails to anticipate.

Thompson discloses a medical data management system for variable data encryption (Col. 4, lines 40-44). A transmitting device, such as a programmer or clinician computer, receives data from an implantable medical device (Thompson, Col. 8, lines 20-26). The transmitting device includes an encryption engine and a decryption engine to process the data for transmission (Thompson, Col. 9, lines 16-29). Once the encryption engine on the transmitting device receives the data, a classifier determines a type of the data, which is then output to a segregator (Thompson, Col. 7, lines 14-16). The segregator separates the data based on predetermined security levels to determine what level of encryption, if necessary, is needed (Thompson, Col. 7, lines 17-20). A key source provides the transmitting device with an encryption key (Col. 8, lines 48-50). Upon determining the level of encryption needed, the data is encrypted with the encryption key and transmitted to a receiving device (Thompson, Col. 7, Lines 23-30). The receiving device decrypts the data with a corresponding decryption key provided by the key source (Thompson, Col. 8, lines 48-50).

In the final Office Action of July 9, 2008, “the route for distribution of the keys by the key source” in Thompson is determined to be “the functional equivalent of the use of a short range or secure [connection] and is a first communication.” Office Action, pages 3-4, pages 8-9, pages 20-21, and pages 24-25. Applicant disagrees and respectfully requests support for the statement.

Further, Applicant asserts that Thompson fails to teach establishing a secure connection through a short range interface from an external source with a key repository, per Claims 1, 30, and 59. Thompson also fails to teach authenticating access to a securely maintained crypto key using a short range

interface, per Claims 60, 69, and 78.

Instead, Thompson teaches a key source to provide an encryption key to a transmitting device and a corresponding decryption key to a receiving device (Thompson, Col. 8, lines 48-59). The key source distributes symmetric or  
5 asymmetric keys (*Id.*). When the encryption algorithms for the keys are known to the public, additional security measures are taken in transmitting the keys from the key source to the transmitting and receiving devices (*Id.*). Although the types of keys provided to the devices are described, Thompson fails to describe or suggest *how* the keys are transmitted to the devices.

10 Thompson is focused on variable encryption and more particularly, a system and method for performing variable encryption of patient data to reduce the amount of bandwidth required. Thus, one skilled in the art would not find that Thompson suggests a short range interface based only on the teaching that a key source provides encryption keys (*Id.*). Therefore, Thompson fails to teach or  
15 suggest such claim elements.

Accordingly, the Thompson reference fails to describe all the claim elements and does not anticipate. Claims 3, 5-10, 17-20, and 27-29 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 31, 32, 34-39, 46-49, and  
20 56-58 are dependent on Claim 30 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 61 and 68 are dependent on Claim 60 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 70 and 77 are dependent on Claim 69 and are patentable for the above-stated reasons, and as  
25 further distinguished by the limitations recited therein. Withdrawal of the rejection is requested.

**Rejections under 35 U.S.C. § 103(a) over Thompson and Lee**

Claims 4, 33, and 79-81 stand rejected under 35 U.S.C. § 103(a) as being obvious over Thompson and further in view U.S. Patent No. 6,442,432, to Lee  
30 (“Lee”). Applicant traverses.

The examiner bears the initial burden of factually supporting any *prima*

*facie* conclusion of obviousness, which includes a clear articulation of the reasons or rationale why the claimed invention would have been obvious. MPEP 2142. Exemplary rationales to support a conclusion of obviousness are listed in MPEP 2143, although the list is not all-inclusive.

- 5           The claims appear to be rejected under the rationale outlining combining prior art elements according to known methods to yield predictable results, which includes *inter alia* “a finding that the prior art included each element claimed, although not necessarily in a single prior art reference, with the only difference between the claimed invention and the prior art being the lack of actual
- 10 combination of the elements in a single prior art reference.” MPEP 2143(A). If any of the findings cannot be made, this rationale cannot be used to support a conclusion that the claim would have been obvious. *Id.*

- Claim 79 recites a secure server to provide identification of and authentication to access an implantable medical device by authenticating access to
- 15 a securely maintained crypto key. Claim 80 recites providing identification of and authentication to access an implantable medical device by authenticating access to a securely maintained crypto key stored on a secure server. Claim 81 recites means for providing identification of and authentication to access an implantable medical device by means for authenticating access to a securely
- 20 maintained crypto key stored on a secure server.

- In contrast, Lee discloses providing data from an implantable medical device to distributed clinicians via an interface medical device (Lee, Abstract). A patient with an implantable medical device situates himself in proximity of the interface medical device, which obtains patient data (Lee, Col. 13, Lines 40-44).
- 25 The interface medical device then transmits the patient data obtained to other medical devices, data communication devices, a central computer, and an expert server through a network connection, such as a local area network or wireless area network (Lee, Col. 10, lines 43-61 and Col. 11, lines 25-44). Encryption is used to authenticate the interface medical device, the implantable medical device, and
- 30 users attempting the access the patient data (Lee, Col. 15, lines 38-42). The encryption covers the entire transmission of the patient data, from the implantable

medical device to the central computer and vice versa (Lee, Col. 16, lines 10-15).

Encrypting data differs from authenticating access to a securely maintained crypto key. Authorization involves determining whether a device is permitted to access data. In contrast, encryption and decryption respectively  
5 involve processes of transforming data to an unreadable state and back into a readable state. Lee describes encryption schemes for the patient data, however, fails to describe *how* the encryption keys are obtained or *on what device* the keys are stored. Thus, Lee teaches encrypting patient data, rather than authenticating access to a securely maintained crypto key on a server.

10 Claim 79 further recites a secure external device to request the crypto key from the secure server via a secure connection based on the identification of and authentication to access the implantable medical device, to receive the crypto key, to commence a data exchange session with the implantable medical device by transitioning to a long range interface upon successful access authentication, and  
15 to transact the data exchange session using the crypto key. Claim 80 recites requesting the crypto key from the secure server via a secure short range connection based on the identification of and authentication to access the implantable medical device. Claim 81 recites means for requesting the crypto key from the secure server via a secure short range connection based on the  
20 identification of and authentication to access the implantable medical device.

Thompson is described above with respect to the anticipation rejection. In the final Office Action of July 9, 2008, “the route for distribution of the keys by the key source” in Thompson is determined to be “the functional equivalent of the use of a short range or secure [connection] and is a first communication.” Office  
25 Action, pages 3-4, pages 8-9, pages 20-21, and pages 24-25. Applicant disagrees and respectfully requests support for the statement.

Applicant asserts that Thompson fails to teach requesting a crypto key via a secure short range interface. Instead, Thompson teaches a key source to provide an encryption key to a transmitting device and a corresponding decryption key to  
30 a receiving device (Thompson, Col. 8, lines 48-59). The key source distributes symmetric or asymmetric keys (*Id.*). When the encryption algorithms for the keys

are known to the public, additional security measures are taken in transmitting the keys from the key source to the transmitting and receiving devices (*Id.*).

Although the types of keys provided to the devices are described, Thompson fails to describe or suggest *how* the keys are transmitted to the devices.

- 5 Thompson is focused on variable encryption and more particularly, a system and method for performing variable encryption of patient data to reduce the amount of bandwidth required. Thus, one skilled in the art would not find that Thompson suggests establishing a short range interface based only on the teaching that a key source provides encryption keys (*Id.*). Therefore, Thompson
- 10 fails to teach requesting a crypto key from a secure server via a secure short range connection based on an identification of and authentication to access an implantable medical device, per Claims 79, 80, and 81.

- Accordingly, a *prima facie* case of obviousness has not been shown. A similar conclusion would adhere under the other exemplary rationales in the KSR
- 15 Guidelines. MPEP 2143. Claim 4 is dependent upon Claim 1 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 33 is dependent upon Claim 30 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

20 **Rejections under 35 U.S.C. § 103(a) over Thompson and Eckmiller**

Claims 11-16, 40-45, 62, 63, 65-67, 71, 72, and 74-76 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Thompson in view of U.S. Patent No. 6,493,587, to Eckmiller et al (“Eckmiller”). Applicant traverses the rejection.

- Adding the teachings of Eckmiller to the teachings of Thompson
- 25 introduces further functionality. However, as discussed above, Thompson fails to anticipate Claims 1, 30, 60, and 69, and the addition of Eckmiller does no more to support an obviousness rejection of dependent Claims 11-16, 40-45, 62, 63, 65-67, 71, 72, and 74-76. Claims 11-16 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited
- 30 therein. Claims 40-45 are dependent on Claim 30 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited

therein. Claims 62, 63, and 65-67 are dependent on Claim 60 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 71, 72, and 74-76 are dependent on Claim 69 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Withdrawal of the rejection is requested.

**Rejections under 35 U.S.C. § 103(a) over Thompson and Wheeler**

Claims 21-26, 50-55, 64, and 73 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Thompson, and further in view of U.S. Patent Application Publication No. 2002/00106913, to Wheeler et al. ("Wheeler").

Applicant traverses.


Adding the teachings of Wheeler to the teachings of Thompson introduces further functionality. However, as discussed above, Thompson fails to anticipate Claims 1, 30, 60, and 69, and the addition of Wheeler does no more to support an obviousness rejection of dependent Claims 21-26, 50-55, 64, and 73. Claims 21-26 are dependent upon Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 50-55 are dependent upon Claim 30 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 64 is dependent upon Claim 60 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 73 is dependent upon Claim 69 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.

Claims 1, 3-30, and 32-81 are believed to be in a condition for allowance. Entry of the foregoing amendments is requested. Reconsideration of the claims, withdrawal of the finality of the Office action, and a Notice of Allowance are earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

Dated: September 2, 2008

By: 

Krista A. Wittman, Esq.  
Reg. No. 59,594

Cascadia Intellectual Property  
500 Union Street, Suite 1005  
Seattle, WA 98101

Telephone: (206) 381-3900  
Facsimile: (206) 381-3999

Final OA Resp